

CLARK HILL

Melissa K. Ventrone
T 312.360.2506
F 312.517.7572
Email: mventrone@clarkhill.com

Clark Hill PLC
130 E. Randolph Street
Suite 3900
Chicago, IL 60601
T 312.985.5900
F 312.985.5999

clarkhill.com

April 25, 2019

Via email to ndag@nd.gov

Attorney General Wayne Stenehjem
Office of the Attorney General
Consumer Protection and Antitrust Division
1050 East Interstate Avenue
Suite 200
Bismarck, North Dakota 58503-5574

Dear Attorney General Stenehjem:

We represent Darlys Anderson Ltd. with respect to a data security incident involving the potential exposure of certain personally identifiable information described in more detail below. Darlys Anderson provides accounting services in Fargo, North Dakota. Ms. Anderson is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On March 12, 2019, Ms. Anderson became aware that an unauthorized user may have accessed its computer network. Ms. Anderson immediately began an investigation to determine whether her systems were secure, and hired an independent computer forensics firm to assist. On March 29, 2019, the forensic investigation determined that the unauthorized user may have accessed folders that contained tax information on her systems. While there is no evidence that the unauthorized user viewed or gained possession of the tax information contained in these folders, Ms. Anderson decided to notify her clients about the incident out of an abundance of caution. Information at risk includes clients' names, addresses, Social Security numbers, bank account information, and other tax related information.

2. Number of residents affected.

Six hundred twenty six (626) North Dakota residents may have been affected and were as notified of the incident. A notification letter was sent to the potentially affected individuals on April 25, 2019 via regular mail (a copy of the form notification letter is enclosed).

Attorney General Wayne Stenehjem
Office of the Attorney General
Consumer Protection and Antitrust Division
April 25, 2019
Page 2

3. Steps taken or plan to take relating to the incident.

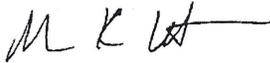
Ms. Anderson took immediate action to address this incident and prevent a similar incident in the future. Steps taken include changing passwords to all employee accounts and implementing additional security protocols for any remote access to the computer system. The notification letter included details about the security incident as well as information about the Federal Trade Commission and the three major credit reporting agencies. The letter offered free credit monitoring and identity theft protection services through ID Experts for one year. Ms. Anderson also provided customers with a toll-free number for any questions.

4. Contact information.

Ms. Anderson takes the security of the information in its control seriously, and is committed to ensuring its customers' information is protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Very truly yours,

CLARK HILL



Melissa K. Ventrone

Enclosure

DARLYS ANDERSON, LTD

Certified Public Accountant

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:

1-800-939-4170

Or Visit:

<https://app.myidcare.com/account-creation/protect>

Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>

<<Address1>> <<Address2>>

<<City>>, <<State>> <<Zip>>

April 25, 2019

Notice of Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing to notify you of a data security incident experienced by Darlys Anderson Ltd. ("Darlys Anderson") that may have impacted your personal information, including your name and Social Security number. We value and respect the privacy of your information, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

What Happened:

On March 12, 2019, we discovered that an unauthorized user may have accessed Darlys Anderson's computer network. We immediately began an investigation to determine whether our systems were secure and hired an independent computer forensics firm to assist. On March 29, 2019, the forensic investigator informed us that the unauthorized user may have accessed folders that contained tax information on Darlys Anderson's systems. While there is no evidence that the unauthorized user viewed or gained possession of the tax information contained in these folders, we wanted to let you know about this incident out of an abundance of caution. Information stored in our system that could be at risk includes your name, address, Social Security number, bank account information if you provided this to us, and other tax related information. To date, there is no indication that any of this information has been misused.

What We Are Doing and What You Can Do:

The security and privacy of your information is important to us, which is why we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-800-939-4170 or going to <https://app.myidcare.com/account-creation/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 8 am - 7 pm Central Time. Please note the deadline to enroll is July 25, 2019.

As noted above, there is no indication that any information has been misused as a result of this incident. However, if you receive a fraudulent deposit from the IRS into your bank account as a result of this incident, the IRS has recommended the following:

1. Do not spend this money, as it must be returned to the IRS.

2. Contact your bank's fraud department and let them know that the money was deposited as a result of a fraudulent tax filing, and that the deposit should be reversed as soon as possible.
3. Do not return the money by check. The most reliable way for the money to be returned and credited to you is to instruct your bank to reverse the deposit.
4. If you have any issues with your bank and the return of the money, please contact Darlys Anderson.

Additionally, if you know or suspect you are a victim of tax-related identity theft, the IRS recommends the following steps:

- If you receive a letter from the IRS, you should follow the instructions on that letter and respond immediately. **The IRS will not contact you via phone.** Additionally, you may be asked to file a paper return for the current filing season.
- If you believe you may be a victim of tax fraud but do not receive a letter from the IRS, you should fill out and submit IRS Form 14039, which is available at [IRS.gov](https://www.irs.gov). Darlys Anderson can provide you with a copy of that form and assist you with filling it out if you would like. If you plan on filing an extension, please contact Darlys Anderson for more information.

If you previously contacted the IRS and did not have a resolution, contact the IRS for specialized assistance at 1-800-908-4490. The IRS has teams available to assist. You may also visit <https://www.irs.gov/Individuals/Identity-Protection> for more information.

We also want you to know that we took immediate action to address this incident to prevent a similar incident in the future. We changed passwords to all employee accounts and devices, and we are in the process of implementing additional security protocols for any remote access to our system, which is currently disabled. We also provided your name and Social Security number to the IRS to help detect possible fraud.

For More Information

If you have any questions or concerns, please call at 1-800-939-4170, Monday through Friday, 8 am - 7 pm Central Time. Your trust is a top priority for me, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,



Darlys Anderson, CPA

U.S. State Notification Requirements

For residents of Hawaii, Michigan, Missouri, New Mexico, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon, Washington, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax
P.O. Box 105139
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 6790
Fullerton, CA 92834
1-800-916-8800
www.transunion.com

You may also obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Colorado, Maryland, Illinois, North Carolina, and Rhode Island:

You can obtain information from the Maryland, North Carolina, and Rhode Island Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Attorney General
Consumer Protection Div.
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Attorney General
Consumer Protection Div.
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Rhode Island Attorney General
Consumer Protection Div.
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue,
NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identityTheft.gov

For residents of Massachusetts:

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via each credit bureau's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is below. As of September 21, 2018, fraud alerts will now last one year, instead of 90 days. Fraud alerts will continue to be free and identity theft victims can still get extended fraud alerts for seven years.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, each credit reporting agency has a dedicated web page for security freezes and fraud alerts or you can request a freeze by phone or by mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request may also require a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. Effective September 21, 2018, placing a freeze on your credit report is now free for all United States citizens.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
www.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed above.